@unipi: centralizzazione del sistema di posta di Ateneo

Simone Spinelli

Università degli Studi di Pisa

Abstract. La pubblica amministrazione sta affrontando un momento di analisi e riorganizzazione delle proprie risorse IT con lo scopo di ottimizzare servizi e costi. Le scelte sulla gestione di servizi strategici come quello di posta elettronica non sono affatto scontate e devono tener conto degli aspetti economici e tecnologici. L'universita' di Pisa ha recentemente migrato i molti sistemi di posta presenti nell'Ateneo su una piattaforma centralizzata che uniforma e migliora i livelli di servizio rispondendo alle esigenze presenti e del prossimo futuro e che sopratutto lascia all'Ateneo pieno controllo dei dati e delle politiche applicate. Si tratta di una soluzione scale-out basata su software opensource interamente progettata e gestita con risorse interne della quale saranno trattati l'architettura, i componenti e i costi.

1. Scenario e obiettivi

La diffusione delle tecnologie di virtualizzazione e del paradigma cloud computing, ha portato profondi mutamenti nel modo di concepire e di utilizzare servizi come la posta elettronica trasformandoli in commodity. Nella pubblica amministrazione, si assiste ad un processo di ristrutturazione dei servizi IT che ha come obbiettivo quello di ottimizzare l'utilizzo delle risorse e di aumentare i livelli di servizio talvolta anche esternalizzandone alcuni come la posta elettronica. Anche l'Università di Pisa, nel corso dell'ultimo anno, ha avviato un processo di razionalizzazione e di normalizzazione che ha coinvolto sia le infrastrutture (di rete, di calcolo e di storage), che i meccanismi di erogazione e gestione dei servizi.

In passato, la gestione dei domini di posta elettronica nell'Ateneo pisano è stata spesso delegata ai singoli dipartimenti. Questo ha portato nel tempo alla proliferazione di una moltitudine di sistemi diversi fra loro in termini di affidabilità, prestazioni e modalità di erogazione del servizio. Per superare questo modello è nato il progetto @unipi, volto a centralizzare il servizio di posta elettronica e a migliorarne e uniformarne le caratteristiche complessive.

Il servizio è rivolto a tutta la comunità universitaria: il personale prima e gli studenti poi. In fase di progettazione sono state considerate le seguenti caratteristiche:

- Scalabilità in termini di numero di utenti e di dimensione della casella;
- 10 Gbyte di spazio per casella;
- Storage con possibilità di tiering;
- Continuità di servizio;
- Gestione dello spam;
- Utilizzo di soli protocolli sicuri e di autenticazione;
- Possibilità di cogestione del servizio con i tecnici dipartimentali;
- Meccanismi di disaster recovery [1];
- Valore giuridico della trasmissione [2].

2. Infrastruttura di computing

I servizi in gestione al settore SerRA si appoggiano su una infrastruttura di macchine virtuali distribuita su due datacenter nel centro cittadino. I siti sono collegati attraverso due anelli in fibra ottica che vengono utilizzati uno per l'esposizione dei servizi e l'altro per il traffico di storage e backup. Alimentazione, collegamenti di rete e storage utilizzano meccanismi di ridondanza e di alta affidabilità in modo da eliminare possibili SPOF. Seguendo la stessa filosofia, anche l'implementazione dei servizi viene fatta utilizzando meccanismi di alta affidabilità.

Per servizi che ospitano dati non ricostruibili, come l'hosting web o i server MDA, sono stati realizzati cluster di macchine virtuali ospitate

Workshop GARR 2014 - Next Network: Costruiamo il futuro della rete - Selected Papers. Roma 2-4 dicembre 2014
ISBN: 978-88-905077-5-5 © 2016 Associazione Consortium GARR

su volumi DRBD [3] replicati in tempo reale sui due datacenter: in ogni momento è possibile far migrare le istanze virtuali da un datacenter all'altro, ottimizzando così l'utilizzo complessivo delle risorse hardware e le prestazioni.
Nel caso di servizi in cui non è necessario preservare i dati o lo stato del sistema, come un DNS cache o una replica LDAP, sono stati utilizzati i meccanismi interni ai protocolli per la replica dei dati e bilanciatori LVS per l'alta affidabilità. Tutto il software utilizzato è opensource: i server fisici e virtuali hanno sistema operativo Linux Debian 6.0 o superiore, la tecnologia di virtualizzazione utilizzata è Xen [4], la replica in tempo reale dei dati viene fatta con DRBD, i cluster sono gestiti con Corosync/Pacemaker [5]e Linux LVS [6] viene utilizzato per i load balancer.

3. Il sistema

Nella progettazione del sistema si è cercato di disaccoppiare le varie componenti funzionali: posta in arrivo e in uscita, mailboxes, webmail, mappe e routing. Questa scelta agevola le operazioni di manutenzione e troubleshooting e permette di utilizzare i meccanismi di alta affidabilità più adatti al singolo servizio. Le componenti individuate sono:

- MTA posta in ingresso;
- MTA posta in uscita;
- MDA;
- Mappe/Routing;
- Webmail.

Al momento la piattaforma @unipi gestisce direttamente le circa 6000 caselle di posta elettronica del personale docente e tecnico amministrativo e il solo traffico di altre 70.000 degli studenti. In totale vengono impiegate 18 macchine virtuali escludendo quelle dedicate al servizio di Identity Management di Ateneo. Uno schema sintetico del sistema è rappresentato in figura 1.

3.1 MTA: posta in ingresso e in uscita

La posta in ingresso viene gestita da quattro server ad egual peso DNS: questo garantisce continuità di servizio e bilanciamento del carico. Il server SMTP utilizzato è Postfix [7].
Le connessioni in ingresso vengono gestite con Postscreen [8] che effettua i controlli di pregreeting (timing e rispetto dei protocolli) e sulle RBL (pesate). Successivamente si passa al blocco SMTP Access di Postfix che effettua i controlli pre-queue (validità di dominio e indirizzo destinatari) e poi a milter-greylist che applica le politiche di greylisting: in caso di assenza di un

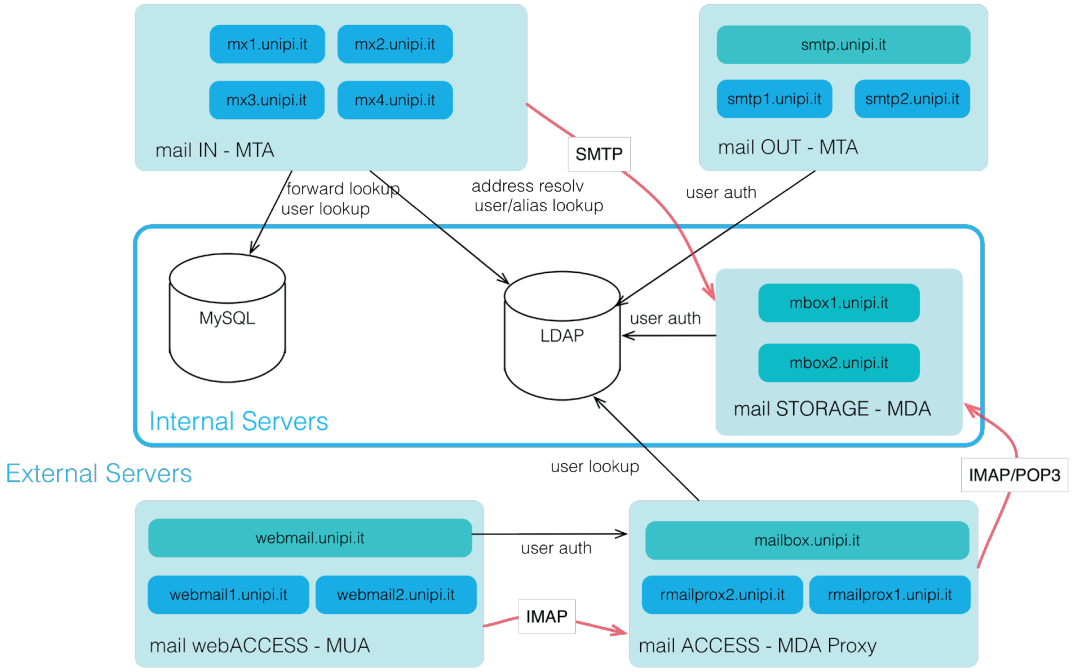

Fig.1 Schema sintetico del sistema

record SPF che indichi la politica da applicare, il server mittente viene messo in una whitelist temporanea, se invece un record SPF è presente, ne viene onorato il contenuto e la connessione viene accettata o rifiutata secondo la corrispondenza fra hostname del server e record SPF. Tutti i client segnalati in RBL che però non superano la soglia di blocco, vengono posti comunque in greylist.

Queste politiche sulle connessioni in ingresso abbattono fortemente il livello di spam e soprattutto il numero di messaggi che vengono analizzati: a fronte di circa un milione di connessioni giornaliere, solo 75.000 messaggi vengono effettivamente analizzati e di questi circa 5.000 vengono marcati o bloccati come spam.
L'analisi dei messaggi per l'applicazione delle politiche anti-spam e antivirus viene effettuata rispettivamente da Spamassassin e Clamav gestiti attraverso AmaVIS. La configurazione di Spamassin è impostata con soglie piuttosto alte: i messaggi vengono segnalati come spam se raggiungono un punteggio di almeno 6 e vengono bloccati con punteggio maggiore di 9. Anche per il learning bayesiano vengono utilizzate soglie alte: vengono considerati spam i messaggi con punteggio maggiore di 12 e ham quelli con punteggio minore di 2,3. È importante sottolineare nuovamente che l'utilizzo di soglie così conservative è possibile grazie all'implementazione di politiche molto rigide in fase di connessione.
Meccanismi antispam e antivirus similari vengono applicati anche sulla posta in uscita: questa scelta aiuta a mitigare il backscattering e ad individuare eventuali account compromessi. Il servizio di posta in uscita è realizzato con due server, esposti all'utenza tramite un bilanciatore e utilizzabili solo in modalità sicura e autenticata. L'utilizzo di un bilanciatore, in questo caso, permette di inserire o rimuovere nodi dal cluster senza disservizio percepibile: sia in caso di operazioni di manutenzione, sia nel caso un server venga compromesso o segnalato in RBL.

3.2 Backend: mappe, routing e identity management

Tutte le informazioni di routing sono mantenute su server specifici: le mappe postfix domain, access e gli alias con destinatari multipli, sono mantenute su un cluster MySQL composto da nodo master e due repliche utilizzate dai server MX: in questo modo si ottiene bilanciamento di carico e alta affidabilità. Un altro cluster MySQL viene utilizzato per i token di Spamassassin e viene popolato e acceduto da tutte le MTA (sia in ingresso che in uscita).

Oltre a fornire il servizio di autenticazione e autorizzazione per l'accesso alla rete e ai servizi, la directory di Ateneo viene utilizzata anche per l'erogazione del servizio di posta. A questo scopo è stata creata una objectClass privata per l'inserimento di attributi specifici per il servizio di posta fra cui indirizzo, alias personali, quota e server MDA di appartenenza.

I server LDAP vengono, quindi, interrogati dai server di posta in ingresso sia per la risoluzione degli alias personali che per la risoluzione degli indirizzi nella forma <username@server_mailbox> (contenuto nell'attributo unipiMailHost) necessaria per la corretta consegna in casella.

Questa soluzione ha permesso di utilizzare differenti server mailbox e quindi di realizzare la scalabilità orizzontale del sistema tramite user sharding.

3.3 MDA: storage e accesso alle caselle

Una volta noto il server MDA di destinazione, il messaggio viene spedito via SMTP al server mailbox di destinazione dove un demone postfix lo consegna a Dovecot [9], l'MDA che si occupa del salvataggio del messaggio in casella.

I server MDA in uso attualmente sono due e sono realizzati con macchine virtuali Xen su volumi DRBD replicati sui due datacenter (con RAID6 locale). Ognuno dei server ha 5TB di spazio disco per le mailbox.

Il frontend per l'accesso alle caselle tramite IMAP/PoP (solo via SSL/TLS) è garantito da un cluster di proxy Dovecot che mascherano all'utente il vero server mailbox di destinazione: il proxy reindirizza la connessione verso il nodo corretto interrogando LDAP (attributo unipiMailHost) e l'utente viene autenticato direttamente sul server di appartenenza. Per questo servizio è stato usato il bilanciamento DNS su due VIP gestiti dal cluster: in caso di fault di un nodo, il vip assegnato migra su uno

dei nodi rimasti. Il servizio di webmail è realizzato utilizzando due server roundcube bilanciati tramite LVS

4. Gestione

L'integrazione con la piattaforma di identity management è essenziale per il provisioning delle risorse: l'attivazione di un indirizzo o un alias personale diventa una operazione che viene fatta sulla piattaforma stessa. Per la gestione di alias a destinazione multipla e per le mappe ospitate su SQL viene utilizzata una semplice interfaccia RubyOnRails. Per il tracciamento dei messaggi e per il trobleshooting è stato realizzato un sysylog server centralizzato che mantiene gli ultimi tre mesi di log, a questo se ne affianca un altro per il mantenimento dello storico (1 anno). L'utilizzo di software aperti permette di utilizzare strumenti standard e facilmente automatizzabili quali ldap-tools, imapsync, rsync, SQL. Le migrazioni dai sistemi dipartimentali a quello centralizzato sono state fatte con questi strumenti che verrano utilizzati in fase di espansione del sistema e che sono usati per realizzare i meccanismi di backup. In questo modo un piccolo set di strumenti standard permette di gestire l'intera piattaforma in tutti i suoi aspetti, dal mantenimento all'espansione. Il sistema in questione è comunque piuttosto complesso e articolato, basti pensare al numero totale di istanze virtuali: gli strumenti di automazione (Rex [10]) e configuration management (Git [11]) hanno svolto e svolgonoo un ruolo essenziale per la gestione, il deploy e lo sviluppo.

5. Analisi dei costi

Sebbene un'analisi dei costi puntuale sia al di fuori degli scopi di questo documento, è possibile fare alcune considerazioni per avere delle indicazioni relative all'investimento iniziale e ai costi nel tempo. Dato che il software in uso non ha alcun costo di licenza, verranno considerati solo i costi relativi all'infrastruttura fisica (server e network) e al consumo energetico. A questi occorre sommare il costo del personale che si può considerare quello di due unità impiegate al 50% (1FTE).

Mentre sono facilmente identificabili i costi relativi allo storage (i dischi sono dedicati), è più difficile calcolare l'incidenza del sistema di posta in termini di risorse di computing e network. Si può però ipotizzare di utilizzare come fattore moltiplicativo il rapporto fra le macchine virtuali dedicate alla posta elettronica e le macchine virtuali attive sull'infrastruttura fisica. Per il network si considera il numero di macchine virtuali attive sull'intera infrastruttura (175), per il computing viene considerato solo il numero di macchine virtuali attive su sistemi fisici sui quali vengono ospitate anche le istanze che compongono il sistema di posta (85).
Fatte queste considerazioni, i risultati sono riassunti dalla tabella seguente:

	Spesa	Incidenza	Spesa posta elettronica
Network	40K €	10%	4K €
Computing	24K €	20%	4.8K €
Infrastruttura fisica	15K €	10%	1.5K €
Totale (escluso storage)	79K €		
Storage			18K €
Totale			28.3K €

Quelli identificati fino ad ora vanno intesi come costi di startup. Occorre ora considerare il tempo di vita del sistema stesso che si può fissare a 5 anni: questo, infatti, è il periodo per il quale l'hardware è coperto da assistenza.

Considerando quindi le spese relative al magazzino hardware (circa 5k euro una tantum) e quelle di assorbimento energetico (circa 6KW per l'intera infrastruttura) si ottiene un costo annuo di circa 1,2 euro/casella. Questo calcolo è fatto considerando le attuali 5.000 caselle attive, ma se il sistema si espandesse a 10.000 caselle, il costo si abbatterebbe a 60cents/casella.

6. Conclusioni e sviluppi futuri

Come per l'investimento fatto a suo tempo sulle infrastrutture di rete, anche sul fronte dei servizi l'Ateneo pisano ha affrontato la sfida con risorse interne: questo ha permesso di mantenere il possesso completo dei dati e del know-how necessario, a fronte di un costo di start-up senza dubbio consistente, soprattutto in termini di im-

pegno professionale, ma che permette nel tempo di crescere secondo le necessità e di mantenere il controllo delle politiche applicate.

Il futuro dell'infrastruttura di posta di Ateneo si sviluppa lungo due direttrici: l'attivazione di nuovi servizi e strumenti che permettano una gestione multi-tenant della piattaforma e lo sviluppo di una soluzione di object-storage basata su CEPH capace di supportare le strutture di ricerca, il personal cloud e un servizio di posta per gli studenti con caratteristiche similari a quello offerto al personale di Ateneo. Lo storage utilizzato per la posta elettronica andrà quindi a rappresentare una parte relativamente piccola di quello utilizzato per la ricerca, la gestione documentale e il personal cloud e questo abbasserà ulteriormente i costi di gestione.

In conclusione, riteniamo che i servizi strategici debbano essere sviluppati e gestiti dalle divisioni IT delle Università. Il valore strategico della posta elettronica non è rappresentato solo dai dati personali contenuti nei messaggi, dalle relazioni che la corrispondenza esprime ma anche, e soprattutto, dalla possibilità di gestire le politiche del servizio, adattandole alle proprie esigenze e mantenendone pieno controllo.

Riferimenti bibliografici

[1] http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/continuita-operativa

[2] http://archivio.digitpa.gov.it/cad/valore-giuridico-della-trasmissione

[3] http://drbd.linbit.com

[4] http://www.xenproject.org

[5] http://clusterlabs.org/doc

[6] http://www.linuxvirtualserver.org

[7] http://www.postfix.org

[8] http://www.postfix.org/POSTSCREEN_README.html

[9] http://www.dovecot.org

[10] http://www.rexify.org

[11] http://git-scm.com

Simone Spinelli
simone.spinelli@unipi.it

Dottore in Ingegneria delle Telecomunicazioni, lavora come System Administrator presso l'Università di Pisa – settore SerRA dal 2002. Si è occupato, tra l'altro, dei servizi di monitoring e di telefonia di Ateneo. Al momento segue lo sviluppo delle infrastrutture di storage e cloud computing.